

QUIZ #1 (open book)

BY using NMap:

1. Scan a single IP address and perform a verbose scan
2. Scan a network range in CIDR notation
3. Scan 7 random hosts
4. Exclude specific hosts
5. Perform a "TCP SYN" Scan on port 80 for specific target
6. Perform a UDP scan on a specific port for specific target
7. Perform a simple list scan for all IPs in the system without actually scanning
8. Perform a ping scan on a single IP
9. Discover the live hosts on your connected network
10. Scan Combination of Individual Ports and Ranges
11. Scan ports from 1 to 100, and exclude port 20 for a specific target
12. Scan Service name https and dns for a specific target
13. Scan by only scanning the most common 100 ports for a specific target
14. Determine the version of the service running on port 80 for a specific target
15. Remote OS detection using TCP/IP stack fingerprinting
16. Limit the number of OS detection probes sent to a target
17. Set the maximum number x of OS detection tries against a target
18. Enable intensity level 9. Higher possibility of correctness